# Windows 認証

2020 年 6 月 19 日

無断複写・転載を禁じます。2011-2020 年 クォリスジャパン株式会社

Qualys および Qualys ロゴは Qualys, Inc. の登録商標です。その他すべての商標は、各所有者に帰属します。

クォリスジャパン株式会社
〒 100-6208
東京都千代田区丸の内 1-11-1
パシフィックセンチュリープレイス 8 階
03-6860-8296

# 目次


**はじめに ..... 4**

**Windows ドメインアカウントの設定 ..... 6**

管理者アカウントの作成 ..... 6
グループポリシーの設定 ..... 6
新規アカウントの機能の検証（推奨） ..... 7

**WMI サービスの設定 ..... 8**

WMI 認証レベルを上げる方法 ..... 8
高レベルの認証が設定されなかった場合 ..... 8

**認証レコードの管理 ..... 9**

Windows レコードの作成 ..... 9
Windows 認証の設定 ..... 10
ログイン資格情報 ..... 14
複数の Windows レコード ..... 16

**付録 A - 非ドメイン（ローカル）スキャン ..... 17**

Windows 2000、2003、XP ..... 17
Windows Vista、2008、2012、2016 ..... 18
Windows 7、8 ..... 21

**付録 B -Windows NT ドメイン ..... 24**

オプション 1 – 管理者グループの使用 ..... 24
オプション 2 – SetACL コマンドラインツールを使用してリモートで ACL を設定 ..... 24

**付録 C - Windows 認証の QID ..... 26**

**サポートへのお問い合わせ ..... 27**

# はじめに

ホスト認証（信頼できるスキャン）を使用すると、スキャン中に各対象システムにログインできます。このため、より精度の高いセキュリティ評価の実施が可能になり、各システムのセキュリティ状態についてより適切に可視化することが可能になります。認証スキャンを実行すると、誤検出を減らし、正確な結果を得ることができます。

## 認証を使用する必要性

脆弱性スキャンでは、認証はオプションですが、使用が推奨されています。コンプライアンススキャンでは、認証は必須です。

## 資格情報の安全性について

資格情報は安全性を確保した状態で扱われ、スキャンの実行中にのみ使用されます。

スキャン機能である Dissolvable Agent とエージェントレス追跡のオプションがユーザによって有効にされており、利用規約に関する承認が与えられていない限り、多くの場合、デバイスに対する変更や書き込みは行われません。

**Dissolvable Agent**: この機能が有効になっている場合、デバイスに対して Dissolvable Agent ファイルが書き込まれ、スキャンの終了時に削除されます。

**エージェントレス追跡**：この機能が有効になっている場合、最初のスキャン時にデバイスに対してホスト ID ファイルが書き込まれます。注記 - サブスクリプションの一次連絡先となるマネージャは、ホスト ID ファイルをホストから削除するクリーンアップアクションをいつでも実行することができます。

**クリーンアップの問題点**：一時ファイルまたは Dissolvable Agent をクリーンアップする前にスキャンが中断されると、ファイルが存在し続ける場合が稀にあります。これは、通常は起こりません。

当社のセキュリティサービスは、スキャン時に昇格された権限でログインを行うために資格情報を使用し、対象からセキュリティ情報を読み取ります。収集された情報を使用することで、スキャナは最大限のセキュリティテストを実行し、設定や構成の大半をチェックします。ここで収集された情報は、スキャンレポートの一部として表示されます。

## 管理者の資格情報を推奨

最も精度の高いセキュリティ評価を行って、ご使用のシステムに推奨される修正を適用するために、管理者権限を使用することをお勧めします。管理者権限を持つアカウントを使用することで、レジストリキー、管理用のファイル共有（C$ など）、実行中のサービスに基づいた情報の収集が可能になります。管理者権限を持たないアカウントを使用することも可能ですが、この場合、スキャンでチェックされる項目が少なくなり、返される結果の正確さと完全性も低くなります。

Windows では、ACL ベースのアプローチが採用されています。各オブジェクト（ファイル、レジストリキー）が、そのオブジェクトに対する特定のアクセスのタイプ（読み取り、書き込みなど）が設定されたアカウントをリストした独自の ACL を持つことができます。アクセスできるオブジェクトが少ないと、“ IPC%$ ” パイプやレジストリ API などを含む各種の認証に失敗することになります。アクセス権がないことは、対応する脆弱性チェック（QID）とコンプライアンスチェック（制御）の失敗に直結します。セキュリティチェックの多くでは、複数のオブジェクトへのアクセスが必要になり、このリストの詳細は、オペレーティングシステムのバージョン、パッチレベル、設定などによって変わります。アクセス権が十分であることを知るための唯一の方法は、スキャンを実行してレポートされたアクセスの失敗を確認することです。

## 使用される認証方式

対象のホストに対し、最も安全性の高い認証方式から順に認証が試行されます。以下の認証方式がサポートされています（安全性の高い順）。

1）AES-128/256 を使用する Kerberos

2）RC4-128 を使用する Kerberos

3）NTLMv2

4）NTLMv1（デフォルトでは無効、Windows 認証レコードで有効にできます）

## 認証スキャンの手順

以下に示す手順は、Qualys スキャンで Windows の信頼できるスキャンを設定する方法です。脆弱性スキャンの場合、対象ホストへの認証はオプションですが、これは推奨されるオプションです。コンプライアンススキャンでは、認証は必須です。

ステップ 1 – 認証のセキュリティサービスで使用される Windows ユーザアカウントを設定します。

ステップ 2 – Qualys を使用して以下を実行します。1）Windows 認証レコードを作成します。2）オプションプロファイルを選択します。脆弱性スキャンの場合は「Authentication」項で “ Windows ” が選択されていることを確認します。3）スキャンを開始します。4）各対象ホストに対して認証が成功したことを確認します。ヒント - 認証レポートを実行して、認証ステータス（「Passed」または「Failed」）を確認します。

# Windows ドメインアカウントの設定

ここでは、認証のためのドメインアカウントの作成方法、アカウントをドメイン管理者グループに追加する方法、グループポリシーの設定方法について説明します。信頼できるスキャンでアカウントを使用する前に、アカウントの機能を検証することをお勧めします。可能な場合、パスワードが有効期限切れにならないようにユーザアカウントを設定します。

## 管理者アカウントの作成

1）管理者権限を持つアカウントでドメインコントローラにログインします。

2）Active Directory Users and Computers MMC スナップインを開きます。

3）“ qualys_scanner ”（または同様の名前）という新しいユーザを作成します。“ qualys ” というアカウントは、Qualys が使用するために予約されており、スキャン中にロックアウトされる可能性があるため、使用しないでください。

4）“ qualys_scanner ” ユーザを選択して、「Properties」を選択します（「Action」 -> 「Properties」）。

5）「Properties」ウィンドウで「Member Of」タブを選択します。「Add」をクリックして、“ qualys_scanner ” ユーザを “ Domain Admins ” グループに追加します。「OK」をクリックして、変更を保存します。

## グループポリシーの設定

ここでは、Windows システムで認証スキャンを行うための、グループポリシー設定に関するベストプラクティスについて説明します。グループポリシーを変更すると、現在のネットワーク設定とセキュリティポリシーによっては、ネットワークの動作に悪影響を与える場合があるため、変更を加える前にネットワーク管理者にお問い合わせください。以下に示すさまざまなグループポリシー設定に関する詳細な説明は、Group Policy Editor を使用する際にオンラインで参照することができます。

**重要！**ローカルネットワーク設定は組織の特定の設定に依存することがあるため、グループポリシーを変更する場合は実施前にネットワーク管理者に相談することを強くお勧めします。Qualys は、ご利用のネットワークでこれらの設定が適切であるかどうかを確認しません。グループポリシーを変更した後、変更がクライアントに反映されるまでには数時間かかることがあります。

### 「Security Options」

「Computer Configuration」→「Windows Settings ?」→「Security Settings」→「Local Policies」→「Security Options」

| | |
|---|---|
| Network access: Sharing and security model for local accounts | Classic |
| Accounts: Guest account status | Disabled（推奨） |
| Network access: Let Everyone permissions apply to anonymous users | Disabled（推奨） |

### 「System Services」

「Computer Configuration」→「Windows Settings」→「Security Settings」→「System Services」

| | |
|---|---|
| Remote registry | Automatic |
| Server | Automatic |
| Windows Firewall | Automatic |

### 「Administrative Templates」

「Computer Configuration」→「Administrator Templates」→「Network」→「Network Connections」→「Windows Firewall」→「Domain Profile」

| | |
|---|---|
| Windows Firewall: Protect all network connections | Disabled（推奨）または Enabled。使用している環境での最適な選択肢はネットワーク管理者が決定します。「Enabled」を選択する場合は、以下の 3 つの設定が必要になります。 |
| Windows Firewall: Allow remote administration exception | Enabled（1） |
| Windows Firewall: Allow file and printer sharing exception | Enabled（1） |
| Windows Firewall: Allow ICMP exceptions | Enabled（2） |

（1）「Allows unsolicited messages from」フィールドには “ * ” を（引用符無しで）入力するか、または Scanner Appliance に割り当てられた IP アドレスを入力します。（2）これは、脆弱性スキャンでは任意ですが、コンプライアンススキャンでは必須です。

## 新規アカウントの機能の検証（推奨）

グループポリシーの設定後、新規の Windows ドメインアカウントの機能を検証して、ポリシーが Windows 認証スキャンに適していることを確認します。

「Start」メニューで「Run」を選択し、cmd.exe と入力して、「OK」をクリックします。以下に示すコマンドを使用して、管理用の共有へのアクセスとレジストリアクセスをテストします。変数部分は、<> で囲んで示してあります。変数部分は適切な値で置き換える必要があります。例えば、<USER> は、jsmith といったユーザ名で置き換えます（括弧は入力しません）。

管理用の共有へのアクセスをテストするため、次のコマンドを実行します。

```
net use Z: \\<IP ADDRESS>\C$ /PERSISTENT:no /USER:<DOMAIN>\<USER>
```

レジストリへのアクセスをテストするため、次のコマンドを実行します。

```
runas /USER:<DOMAIN>\<USER> "cmd /k reg.exe query \\<IP
ADDRESS>\HKLM\Software"
```

注記 : “ query ” と \\<IP ADDRESS> の間にはスペースがあります。

# WMI サービスの設定

コンプライアンスチェックの一部では、コンプライアンス評価を正常に実行するために WMI サービスへの安全なアクセスが必要になります。このため、認証レベルを「Packet Privacy」まで上げて、WMI サービスが安全に実行されるように設定することをお勧めします。

次の名前空間と関連するコントロールをスキャンするには、高レベルでの認証が必要になります。

名前空間 : **root\cimv2\security\microsofttpm**

CID 11279 - Windows 上の「Trusted Platform Module (TPM)」のステータス（「Activated」）

CID 11287 - Windows 上の「Trusted Platform Module (TPM)」のステータス（「Enabled」）

CID 11288 - Windows 上の「Trusted Platform Module (TPM)」のステータス（「Owned」）

名前空間 : **root\CIMV2\TerminalServices**

CID 11478 - リモートデスクトップ接続権限が付与されているグループおよびユーザアカウントの現在のリスト

## WMI 認証レベルを上げる方法

上で説明した名前空間およびコントロールについてスキャンを実行する各ホストに対して、次のコマンドを実行する必要があります。

```
winmgmt /standalonehost 6
```

次に Winmgmt サービスを再起動します。

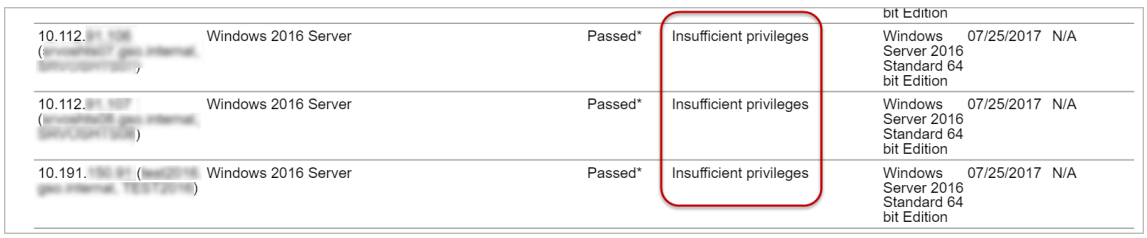
```
net stop winmgmt
net start winmgmt
```

認証レベルの詳細については、https://msdn.microsoft.com/en-us/library/aa393972(v=vs.85).aspx を参照してください。

## 高レベルの認証が設定されなかった場合

高レベルの認証を必要とする名前空間およびコントロールのスキャン時に、「Insufficient Privileges」（特権が不十分）または WMI クエリの失敗が表示されることがあります。

Windows 認証レポートのエラーの例を示します。



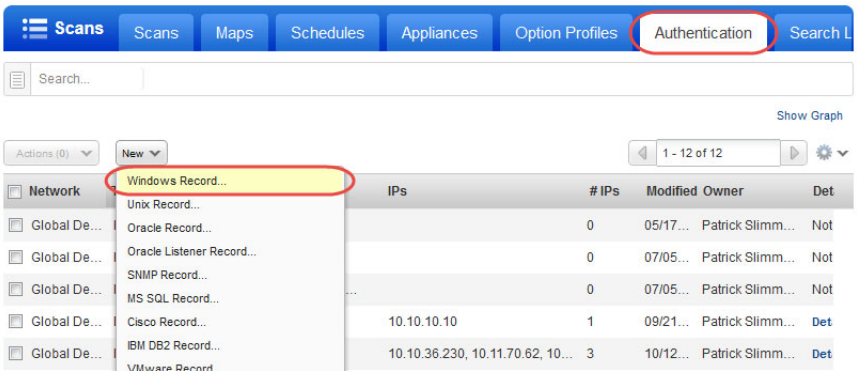
| | | | | |
|---|---|---|---|---|
| 10.112.[redacted] | Windows 2016 Server | Passed* | Insufficient privileges | Windows Server 2016 Standard 64 bit Edition 07/25/2017 N/A |
| 10.112.[redacted] | Windows 2016 Server | Passed* | Insufficient privileges | Windows Server 2016 Standard 64 bit Edition 07/25/2017 N/A |
| 10.191.[redacted] | Windows 2016 Server | Passed* | Insufficient privileges | Windows Server 2016 Standard 64 bit Edition 07/25/2017 N/A |

# 認証レコードの管理

Qualys のサービスがスキャン時に Windows ホストの認証を得られるように Windows レコードを作成します。各レコードでは、1）ログインするための資格情報、2）資格情報を使用してログインを行う IP アドレスが識別されます。

## Windows レコードの作成

「Scans」→「Authentication」を選択し、「New」→「Operating Systems」→「Windows」を選択します。




### レコードを作成するパーミッションを持つユーザ

マネージャは、認証レコードを追加することができます。ユニットマネージャにも、この権限が与えられることがあります。スキャナに対しては、サブスクリプションで許可するように設定されている場合にのみ、このパーミッションが付与されます。

### 複数のレコードがある場合に使用される資格情報

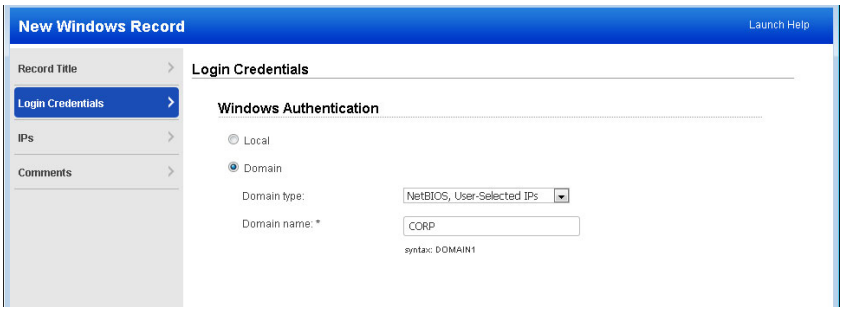
複数のレコードがある場合は、スキャン時に各対象ホストとレコードが 1 つずつ照合されます。「ログイン資格情報」を参照してください。

### 作成後の Windows レコードの編集

レコードは、ログイン資格情報、対象ホストやその他の設定を変更するためにいつでも編集できます。元の設定を残しておくために、変更を行う前にレコードのコピーを作成することもできます。「Scans」→「Authentication」を選択して、編集する Windows レコードを見つけます。リストにあるレコードの上にマウスポインタを置いて、「Quick Actions」メニューから「Edit」を選択します。

マネージャ以外のユーザがレコードを編集する場合の注記 - 表示するパーミッションが付与されているレコードの IP のみが表示されます。レコードには実際にはより多くの IP が含まれていることがあり、これに変更を加えると、表示されていないホストも含めて、レコードに定義されているすべてのホストに影響があります。

# Windows 認証の設定




## ローカル認証

ローカル認証を選択した場合、認証は、「IP」項目に入力したホストのローカルで実行されます。アカウント要件については、「付録 A - 非ドメイン（ローカル）スキャン」を参照してください。

## ドメイン認証

ドメインタイプを選択し、ドメイン名を入力します。

「NetBIOS, User-Selected IPs」- こちらを選択すると、ドメイン設定にある IP アドレスへの認証に NetBIOS が使用されます。レコードの「IPs」項に IP を入力します。この方式でドメイン（ツリー）全体に対して 1 つの認証レコードを定義できます。

「NetBIOS, Service-Selected IPs」- こちらを選択すると、ドメインに保存されている資格情報を使用するドメインのホストの認証に NetBIOS が使用されます。信頼関係が存在し、アカウントのパーミッションが正しく伝播されていれば、同じドメインのメンバーでないホストの認証が可能です。

「Active Directory」- こちらを選択すると、フレームワーク内の特定のドメインのホストの認証に Active Directory フォレストが使用されます。完全修飾ドメイン名（FQDN）の入力が必要です。「Follow trust relationships」を選択し、信頼関係が存在する場合は、レコードで定義したドメインと信頼関係のある他のドメインのホストの認証が行われます。

## 信頼関係

### 信頼関係のサポート

Windows ドメインのログインでは、信頼関係がサポートされます。つまり信頼関係がある場合は、あるドメインに格納された資格情報を使用して、別のドメインに格納された 1 つ以上のホストの認証が行えます。これは、パススルー認証を使用して、スキャン対象によって自動的に行われます。

### 信頼関係に従う場合

「Follow trust relationships」設定（Active Directory ドメインタイプで使用可能）は、すべてのドメインが単一の場所（1 か所のオフィスなど）にある、小規模から中規模のビジネスを想定したものです。この設定は、ドメイン間にファイアウォールがある、数百ものドメインが多くの場所に拡散するエンタープライズの顧客を想定したものではありません。

この設定が有効である場合、認証レコードで使用されている信頼関係のあるドメインのフォレストにおいて、すべてのドメインにおけるすべてのドメインコントローラにスキャナがアクセスできる必要があります。これらのドメインコントローラへの接続、またはこれらのドメインを解決する DNS サーバへの接続がファイアフォールによってブロックされると、認証失敗の原因になります。

## NetBIOS と Active Directory の比較 - 一般的な使用例

レコードでどちらのオプションを選択すればよいのか確信が持てない場合は、以下を参考にしてください。一般に、名前のマッピングに関係するドメイン間の設定方法において、NetBIOS よりも Active Directory レコードの方が好まれています。NetBIOS レコードの場合、Kerberos プロトコルを使用できない状況が多くなります。NetBIOS および Active Directory のドメイン間では、手動による設定がサポートされています。

以下の使用例とレコード設定を確認して、どちらを選択するのかを決めてください。

### IP ベースの認証

ドメインタイプ : NetBIOS, User-Selected IPs
ドメイン名 : DOMAIN
ユーザ名 : USER

### ホストベースの認証

ドメインタイプ : NetBIOS, Service-Selected IPs
ドメイン名 : DOMAIN
ユーザ名 : USER

### NTLM のサービスベースの認証（Kerberos 使用不可）

信頼関係がない場合
“ DOMAIN ” を “ domain.foo.com ” にマッピングできる場合、Kerberos へのアップグレードが試みられます。

ドメインタイプ : NetBIOS, Service-Selected IPs
ドメイン名 : DOMAIN
ユーザ名 : USER

### NTLM のサービスベースの認証（Kerberos 使用不可）

手動で設定された信頼関係がある場合
この場合は Kerberos へアップグレードできません。

ドメインタイプ : NetBIOS, Service-Selected IPs
ドメイン名 : TARGETDOMAIN
ユーザ名 : USERDOMAIN\USER

### Kerberos のサービスベースの認証

信頼関係がない場合
この場合は常に、最初に Kerberos が試されます。

ドメインタイプ : Active Directory
ドメイン名 : domain.foo.com
ユーザ名 : USER
「Follow trust relationships」設定 : OFF

### Kerberos のサービスベースの認証

手動で設定された信頼関係がある場合
この場合は常に、最初に Kerberos が試されます。
ドメイン間の認証があるエンタープライズ組織にお勧めします。

ドメインタイプ : Active Directory
ドメイン名 : targetdomain.foo.com
ユーザ名 : USER@userdomain.foo.com
「Follow trust relationships」設定 : OFF

### Kerberos のサービスベースの認証

信頼関係の自動検出がある場合
中小規模のビジネスの場合にのみお勧めします。

ドメインタイプ : Active Directory
ドメイン名 : userdomain.foo.com
ユーザ名 : USER
「Follow trust relationships」設定 : ON

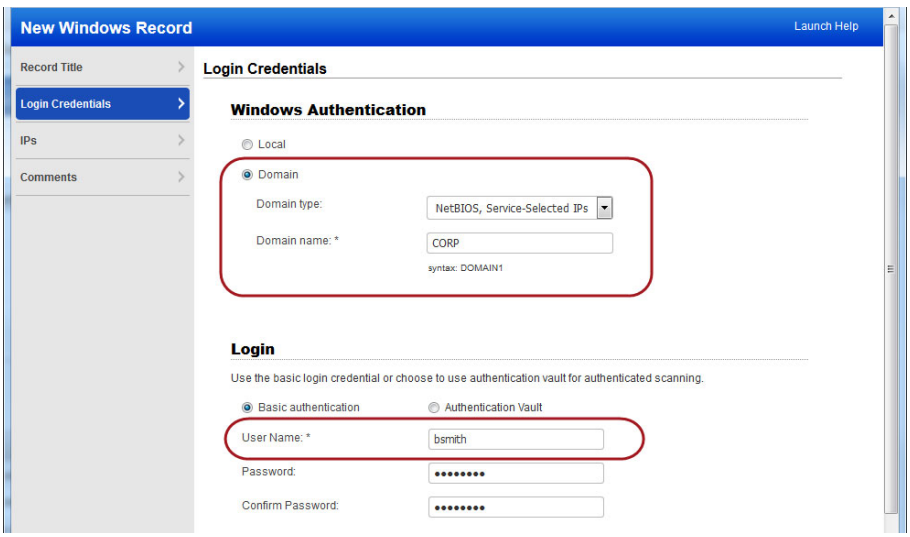
## 「NetBIOS, Service-Selected IPs」の例

Service-Selected IP で Windows ドメイン認証オプションを使用する場合は、以下のシナリオで認証方法を確認してください。

### ホストがドメインのメンバーである場合

セキュリティサービスは NetBIOS を使用して、ユーザ指定のドメインのホストへの認証を行います。資格情報は、このドメインに格納されたものを使用します。信頼関係が存在し、アカウントのパーミッションが正しく伝播されていれば、同じドメインのメンバーでないホストの認証が可能です。

例 : CORP は最上位のドメインです。アカウントの資格情報は、CORP ドメインに格納されます。



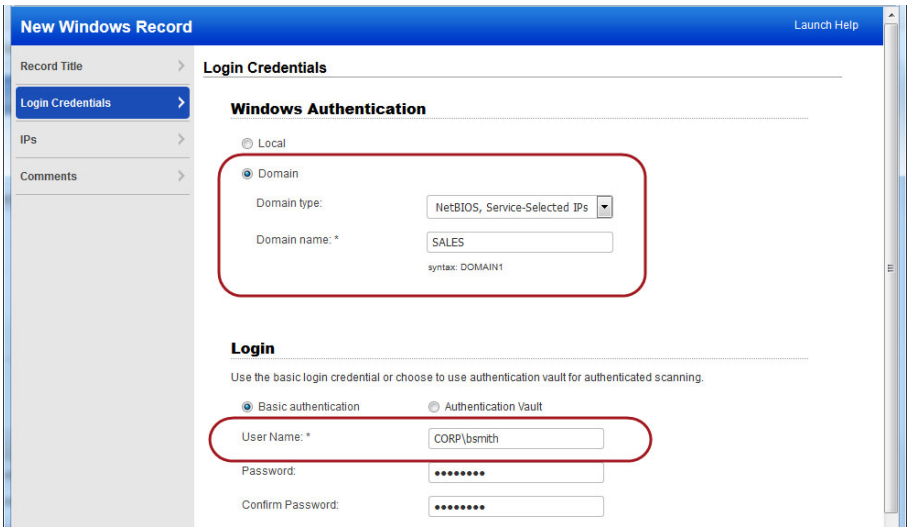
### ホストがドメインのメンバーでない場合

このオプションは、アカウントの資格情報のあるドメインと、対象ホストが存在する子ドメインの間に正しい信頼関係がある場合に使用できます。アカウントパーミッションがホストのドメインに正しく伝播されている必要があります。

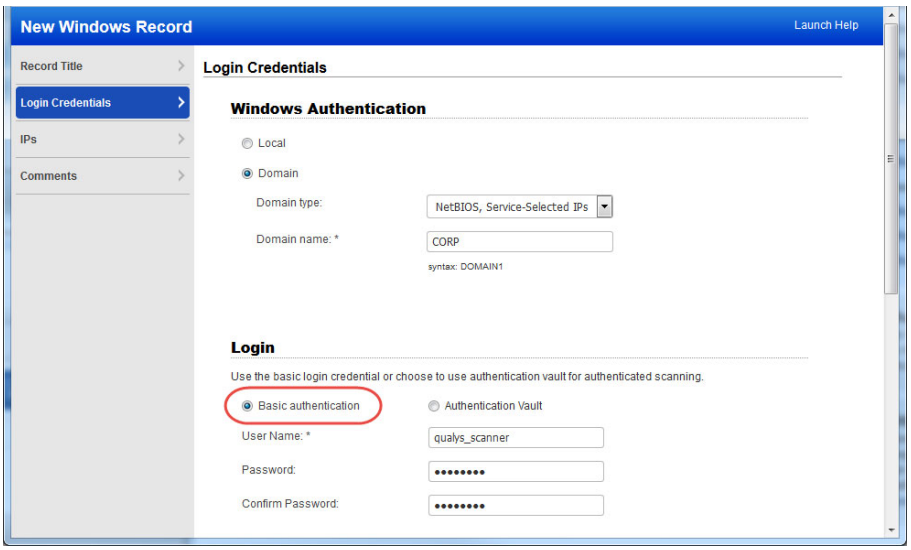
「User Name」フィールドで、“ domain\user ” という形式を指定します。注記 : “ user@domain ” という形式はサポートされていません。“ domain\user ” 形式を使用すると、スキャン対象ホストがあるドメインのメンバーであり、認証資格情報が他のドメインに保存されている場合に、信頼できるドメインごとに Windows 認証レコードを作成することができます。

「Domain Type」ドロップダウンで、「NetBIOS 、Service-Selected IPs」を選択します。スキャン対象ホストを識別するためのドメイン名を入力します。「User Name」フィールドに、値 “ domain\user ” を入力します。ここで、“ domain ” は、認証資格情報を含むドメインで、“ user ” は別のドメインに保存されたこれらの資格情報のアカウント名です。

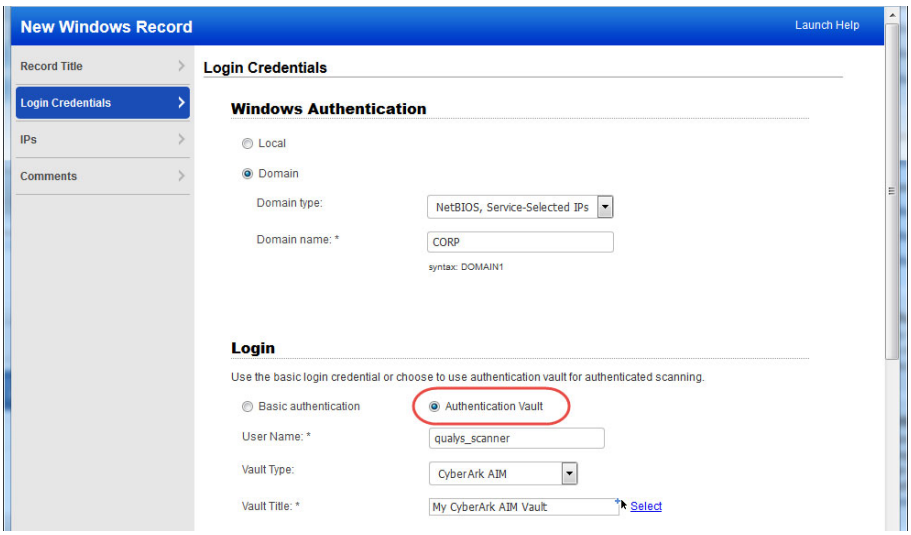
例 ：適切な信頼関係が存在する場合、CORP は、最上位のドメインです（フォレストのルート）。アカウント “ vsmith ” の資格情報は、最上位ドメイン “ CORP ” に保存されます。対象ホストは、子ドメイン “ SALES ” のメンバーです。「User Name」フィールドに “ CORP\vsmith ”、「Domain Name」フィールドに “ SALES ” を入力します。



# ログイン資格情報




「Basic Authentication」を選択した場合は、スキャン時の認証で使用されるユーザ名とパスワードを入力します。




組織がパスワードをサードパーティのパスワードマネージャに保存している場合は、保存先のパスワードにアクセスできます。これには、アカウントに Vault 設定を作成する必要があります。Vault 設定を使用して、パスワードマネージャアプリケーションにアクセスすることが可能になり、レコード設定からスキャン対象のホストのパスワードを取得する方法が判明します。

「Scans」→「Authentication」→「Vaults」に移動して、使用している Vault システムを設定します。次にレコードで「Authentication Vault」を選択し、Vault 名を選択します。

## 認証プロトコル

Qualys のスキャナは、レコードで選択されている認証プロトコルから、安全性の高いプロトコルを順に 1 つずつ使用して、対象ホストへの認証を試みます。ドメインレベルの認証では 3 種類のプロトコルがすべてサポートされています。ローカルホストの認証では、NTLMv2 および NTLMv1 プロトコルがサポートされています。

## IPs

このレコードに定義されているログイン資格情報を使用するために、認証を受ける Windows ホスト（IP）を選択します。各 IP は、1 つの Windows レコードに含めることができます。ドメインレベルの認証では、ドメインタイプ「NetBIOS, User-Selected IPs」が使用されている場合、IP のみを選択することができます。この項で指定されているすべての IP がドメイン設定に含まれている必要があります。

## SMB オプション

「SMB signing required」- このオプションは、デフォルトでは選択されていません。つまり SMB 署名は必須ではありません。これが推奨設定です。チェックが外されていると、対象ホストでの SMB 署名の設定方法にかかわらず、Windows の任意のバージョンで認証が可能です。ただし、中間者（MITM）攻撃に対しては、無防備になります。

このオプションが選択されている場合、Windows の各対象ホストについて、ローカルポリシーまたはグループポリシーの設定によって SMB 署名がサポートされている必要があります。SMB 署名が対象ホストで無効化されている場合、認証に失敗するためホストはスキャンされません。このオプションは MITM 攻撃に対して保護を行うものですが、一部のホストについては認証ができなくなります。

「Minimum SMB version」- SMB プロトコルの最小バージョン（1、2.0.2、2.1 など）を選択してください。Windows の各対象ホストにこれ以上のバージョンがあることが必要になります。認証の対象に、それより前の SMB プロトコルがある場合、認証に失敗し、ホストはスキャンされません。

## エージェントレス追跡

エージェントレス追跡機能は、IP アドレス（または DNS 名や NetBIOS 名）に依存してホストを識別する代わりに、ホスト ID によってホストの追跡を可能にする機能です。これは、複数の IP アドレスを使用してシステムをスキャンし、一意のホスト ID にすべての脆弱性をまとめるために結果を解析するユーザに対してスキャンオプションを提供することになります。

レコードにあるホストをホスト ID によって追跡するには、「Enable agentless tracking」オプションを選択します。スキャンプロセスの実行中、対象の各ホストには一意のホスト ID がサービスによって割り当てられます。

このホスト ID は、ホストのローカルファイルシステムの次のレジストリに保存されます。

レジストリキー : HKLM\SOFTWARE\Qualys

値名 : HostID

詳細については、Qualys のオンラインヘルプを参照してください。

# 複数の Windows レコード

Windows 認証レコードは必要なだけいくつでも設定できます。各 Windows ホストは、常に 1 つの Windows レコードとの照合が試みられます。照合するものが見つかった場合は、この照合したレコードをホストの認証に使用し、他に照合する可能性があるレコードについては検索を中止します。

複数の Windows レコードがある場合、ホストを Windows レコードと照合するときに適用される順序は、次に示すいくつかのことに依存します。

## レコードタイプが評価される順序

1)「NetBIOS, Service-Selected IPs」に設定されているレコード

サービスにより選択された IP が設定されている Windows レコード(「Domain: NetBIOS, Service-Selected IPs」に設定されているレコード)が参照され、これらのいずれかのレコードのドメインにホストが登録されているかどうかが調べられます。一致が見つかった場合、認証にはそのレコードの資格情報が使用されます。

2)「NetBIOS, User-Selected IPs」に設定されているレコード

ユーザが対象ホストの IP を設定した Windows レコード(「Domain: NetBIOS: User- Selected IPs」と「Local」が有効になっているレコード)が参照され、これらのレコードのいずれかにホストが含まれているかどうかが調べられます。最初にドメインレコード、次にローカルレコードで照合が行われます。サービスにより選択された IP レコードの資格情報がホストへの認証に使用され、認証が失敗した場合は、ユーザによりローカル認証専用として選択された IP レコードにそのホストが含まれているかどうかが調べられます。一致が見つかった場合、認証にはそのレコードの資格情報が使用されます。

3)「Active Directory」に設定されているレコード

「Active Directory」に設定されている Windows レコードが調べられ、それぞれに定義されている完全修飾ドメイン名(FQDN)で見つかったホストに対して認証が試行されます。

## 管理者アカウントとその他のアカウント

管理者アカウントが最初に設定されたレコード

最初に、管理者アカウントが設定された Windows レコードで、1)「NetBIOS, Service-Selected IPs」に設定されているレコード、2)「NetBIOS, User-Selected IPs」に設定されているレコード、3)「Active Directory」に設定されているレコードの順序で、ホストとの照合が行われます。

その他のアカウントが設定されたレコード

管理者アカウントが設定されたレコードで、ホストと照合しなかった場合、その他のアカウントが設定された Windows レコードで、1)「NetBIOS, Service-Selected IPs」に設定されているレコード、2)「NetBIOS, User-Selected IPs」に設定されているレコード、3)「Active Directory」に設定されているレコードの順序で、ホストとの照合が行われます。

# 付録 A - 非ドメイン（ローカル）スキャン

ローカルシステムで信頼できるスキャンを準備する際に、システムがドメインに参加していない場合は、次のシステム設定が有効であることを確認してください。これらの設定が有効になっていない場合、セキュリティサービスはネットワーク上の対象ホストに対し、Windows の信頼できるスキャンを実行できません。

Windows 2000、2003、XP | Windows Vista、2008、2012、2016 | Windows 7、8

## Windows 2000、2003、XP

### ローカルアカウント

管理者グループ内のローカルアカウントを使用する必要があります。

### サーバサービスの有効化

サーバサービスは、通常は有効になっています。無効になっている場合は、ポリシーまたはスクリプトを通じて有効にすることができます。信頼できるスキャニングに必要なファイルとプリンタの共有は、サーバサービスが有効になっている場合にのみ機能します。

### ネットワークインタフェースでのファイルとプリンタの共有の有効化

スキャンされるすべてのホストのネットワークインタフェースで、ファイルとプリンタの共有が有効になっている必要があります（デフォルトでは有効になっています）。ネットワークインタフェースのプロパティから手動で有効にするか、“ netset.exe ” や “ netcfg.exe ” などのツールを用いて、スクリプトから有効にします。Netset.exe とは、ネットワークインタフェースの設定変更をサポートする、Windows のコマンドラインツールです。Snetcfg.exe とは、Microsoft 開発キットツールです。Windows 2000 および Windows XP 対応の、snetcfg のコンパイル済みバージョンもあります。

### 簡易ファイルの共有（Simple File Sharing: SFS）の無効化 : Windows XP

Windows XP システムをスキャンするには、簡易ファイルの共有（SFS）を無効にする必要があります。Windows XP Pro システムがドメインに加わった段階では、SFS はデフォルトでは無効になっているため、エンタープライズネットワークの Windows XP Pro システムで信頼できるスキャンをサポートするために設定を変更する必要はありません。ユーザが SFS を有効にしていることもあるので、グループポリシーなどの方法により、無効になっていることを確認する必要があります。

ドメインに追加されていない Windows XP Home システムまたは Windows XP Pro システムをスキャンする場合、これらのシステムで SFS を無効化する必要があります。

このオプションを、マシン単位で手動で無効にすることも可能です。これをローカルマシンで行うには、Windows エクスプローラで、「ツール」→「フォルダ オプション」→「表示」を開きます。「詳細設定」で、「簡易ファイルの共有を使用する ( 推奨 )」設定を解除し、「OK」をクリックします。

### リモートレジストリサービスの有効化

Windows の信頼できるスキャンを実行するには、スキャンサービスがシステムレジストリにアクセスする必要があります。このアクセスを可能にするために、リモートレジストリサービスが有効になっている必要があります。これを確認するには、「コントロール パネル」→「管理ツール」→「サービス」に移動し、サービスが実行中で自動起動が設定されていることを確かめます。

## Windows ファイアウォールでのリモート管理の許可 : Windows 2003、XP

Windows ファイアウォール（使用されている場合）を通じたアクセスを可能にするには、Windows ファイアウォールでリモート管理の例外を設定する必要があります。この設定は、グループポリシーを使用し、次の場所で見つけることができます。

Computer Configuration\Administrative Templates\Network\Network Connections\Windows Firewall\Standard Profile（使用中のコンピュータが Windows ドメインのメンバーである場合は、「標準プロファイル」を「ドメイン プロファイル」に変更します）。

コントロールパネルからファイアウォールを管理している場合は、TCP ポート 135 および 445 を有効にします。

# Windows Vista、2008、2012、2016

## Windows ファイアウォールの設定

各対象ホストに対し、有効にするべき Windows ファイアウォール設定がいくつかあります。

### ステップ 1: 「ファイルとプリンターの共有」トラフィックの許可

非ドメインプロファイルに関連するファイアウォールルールをアクティブ化し、ファイルとプリンタの共有のトラフィックを許可します。

1）「コントロール パネル ホーム」ウィンドウを開きます。

2）次のいずれかを実行します。

- Windows Vista および 2008 の場合 : 「セキュリティ」を選択し、「Windows ファイアウォールによるプログラムの許可」リンクをクリックします。

- Windows 2012 および 2016 の場合 : 「システムとセキュリティ」→「Windows ファイアウォール」を選択して、「Windows ファイアウォールによるプログラムの許可」リンクをクリックします。

3）「ファイルとプリンターの共有」チェックボックスを選択します。

4）「OK」をクリックします。

### ステップ 2: Scanner Appliance トラフィックの許可

デフォルトでは、非ドメインプロファイルの場合、ファイアウォールルールが有効になっていても、Windows システム（Vista、2008、2012、または 2016）は自身のローカルサブネット外からのトラフィックを許可しません。そのため、Scanner Appliance の IP アドレスまたはサブネットも指定する必要があります。

1）「スタート」→「コントロール パネル」→「システムとメンテナンス」→「管理ツール」に移動します。

2）次のいずれかを実行します。

- Windows Vista、2008、2016 の場合 : 「セキュリティが強化された Windows ファイアウォール」に移動します。

- Windows 2012 の場合 : 「Windows ファイアウォール」→「詳細設定」に移動します。

3）「受信の規則」をクリックします。

4)「ファイルとプリンターの共有」グループで緑のチェックマークがある各エントリ（Vista、2008 および 2012）および、「リモート管理」グループで緑のチェックマークがある各エントリ（Vista および 2008）について、a）エントリで右クリックして「プロパティ」を選択し、b)「スコープ」タブを選択し、c)「任意の IP アドレス」を選択するか、「追加」ボタンをクリックして、対象ホストをスキャンするように設定されている Scanner Appliance の IP アドレス（またはサブネット）を追加という手順を実行します。

5)「OK」をクリックします。

## ファイル共有の有効化

対象ホストごとに、ファイル共有を有効にする必要があります。「コントロール パネル ホーム」ウィンドウに移動し、次の手順に従います。

### Windows Vista および 2008 の場合 :

1)「ネットワークとインターネット」項目で、「ファイルの共有の設定」リンクをクリックします。

2)「ネットワークと共有センター」ウィンドウで、「ファイル共有」がオン、「パブリック フォルダ共有」がオフになっていることを確認します。

### Windows 2012 および 2016 の場合 :

1)「ネットワークと共有センター」で、「共有の詳細設定の変更」リンクをクリックします。

2）現在のネットワークプロファイルの共有オプションを変更します。

- 非ドメインターゲットの場合は、「ゲストまたはパブリック」を選択します。

- ドメインターゲットの場合は、「プライベート」を選択します。

3）設定で、ネットワーク検出と、ファイルとプリンタの共有がオンになっていることを確認します。

4）すべてのネットワークについて、「パブリック フォルダ共有」をオフにし、「パスワード保護共有」をオンにします。

## リモートレジストリサービスの有効化

Windows の信頼できるスキャンを実行するには、サービスがシステムレジストリにアクセスできる必要があります。このアクセスを可能にするには、リモートレジストリサービスが開始されている必要があります。

1)「コントロール パネル」→「コントロール パネル ホーム」→「システムとメンテナンス」→「管理ツール」→「サービス」を選択します。

2）リモートレジストリサービスを開始します。このサービスを「自動」に設定して、再起動時にサービスが自動的に開始されるように設定することもできます。

## ユーザアクセス制御（UAC）の設定

UAC を設定する必要があります。設定には、1）リモート UAC 設定の変更、2）UAC ポリシーの無効化という 2 つの方法があります。

### 方法 1: リモート UAC の設定

1)「管理者として実行」モードでレジストリ エディター（regedit.exe）を開始し、必要であれば管理者承認を付与します。

2）HKEY_LOCAL_MACHINE ハイブに移動します。

3）SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System キーを開きます。

4）次のプロパティを指定して新しい DWORD（32 ビット）値を作成します。

名前 : LocalAccountTokenFilterPolicy
値 : 1

5）レジストリ エディターを閉じます。

警告 : DWORD（32 ビット）と QWORD（64 ビット）のデータタイプの値は、64 ビットバージョンの Windows ではメニューで隣り合わせに位置しています。そのため、間違ったデータタイプを選択するミスが発生しやすくなっています。データタイプは、DWORD（32 ビット）であることが必要です。QWORD（64 ビット）を選択して、値を 1 に設定しても、リモート UAC は有効になりません。

システムの再起動またはサーバサービスの再始動の要請には疑問の余地があります。一部のドキュメントで推奨されているのにもかかわらず、レジストリでリモート UAC を無効にすると、これはすぐに反映されて、スキャン中に ADMIN$ へのリモートアクセスが許可されます。

### 方法 2: UAC ポリシーの無効化

「コントロール パネル ホーム」ウィンドウに移動し、次の手順に従います。

#### Windows Vista、2008、2016 の場合 :

1)「ユーザーアカウントの追加または削除」をクリックします。

2）ユーザアカウントを選択します。

3）ユーザアカウントの下のリンク「メインのユーザー アカウントのページに移動」をクリックします。

4)「ユーザーアカウントの変更」ページで、「セキュリティ設定の変更」をクリックします。

5)「ユーザー アカウント制御 (UAC) を有効にして、お使いのコンピュータをより安全にします」ページで、「ユーザー アカウント制御 (UAC) を使ってコンピュータの保護に役立たせる」チェックボックスをオフに（クリア）し、「OK」をクリックします。

6）コンピュータを再起動します。

#### Windows 2012 の場合 :

1）ユーザアカウントをクリックします。

2）ユーザアカウント制御の設定を変更します。

3）タブを「アプリがコンピューターに変更を加えようとする場合のみ通知する ( デスクトップを暗転しない )」に設定します。

4）コンピュータを再起動します。

### UAC に関する情報

Qualys の文書『Qualys Authenticated Scanning - Microsoft Windows User Access Control (UAC)』を確認してください。アカウントにログイン後、「Help」→「Resources」に移動して最新版をダウンロードしてください。

# Windows 7、8

## Windows ファイアウォールの設定

各対象ホストに対し、有効にするべき Windows ファイアウォール設定がいくつかあります。まず、非ドメインプロファイルに関連するファイアウォールルールをアクティブ化し、ファイルとプリンタの共有のトラフィックを許可します。次に、アクティブ化された各ルールに対して Scanner Appliance の IP アドレスまたはサブネットを追加し、Scanner Appliance のトラフィックがホストに到達できるようにします。

「ファイルとプリンターの共有」トラフィックを許可します。次の手順に従います。1）「コントロール パネル ホーム」ウィンドウに移動し、2）「システムとセキュリティ」→「Windows ファイアウォール」で「Windows ファイアウォールによるプログラムの許可」をクリックし、3）「ファイルとプリンターの共有」チェックボックスを選択して、4）「OK」をクリックします。

デフォルトでは、非ドメインネットワークプロファイルシステムは、ファイアウォールルールが有効になっている場合であっても、自身のローカルサブネット以外からのトラフィックを許可しません。そのため、Scanner Appliance の IP アドレスまたはサブネットが含まれるようにファイアウォールルールの範囲を変更する必要があります。

Scanner Appliance のトラフィックを許可するには、次の手順に従います。

1）「スタート」→「コントロール パネル」→「システムとセキュリティ」→「管理ツール」にある「セキュリティが強化された Windows ファイアウォール」に移動します。

2）「受信の規則」をクリックします。

3）「ファイルとプリンターの共有」グループで緑のチェックマークがある各エントリについて、a）エントリで右クリックして「プロパティ」を選択し、b）「スコープ」タブを選択し、c）「任意の IP アドレス」を選択するか、「追加」ボタンをクリックして対象ホストをスキャンするように設定されている Scanner Appliance の IP アドレス（またはサブネット）を追加という手順を実行します。続けて「OK」をクリックします。

## ファイル共有の有効化

次の手順に従って、対象ホストごとにファイル共有を有効にする必要があります。1）「コントロール パネル ホーム」ウィンドウに移動し、2）「ネットワークとインターネット」→「ホームグループ」で「共有の詳細設定の変更」リンクをクリックし、3）現在のネットワークプロファイルの共有オプションを変更します。非ドメインターゲットの場合は、「ホームまたは社内」を選択します。ドメインターゲットの場合は、「ドメイン」を選択します。設定で「ファイル共有」がオン、「パブリック フォルダ共有」がオフになっていることを確認します。

## リモートレジストリサービスの有効化

Windows の信頼できるスキャンを実行するには、スキャンサービスがシステムレジストリにアクセスできる必要があります。サービスがシステムレジストリにアクセスできるようにするには、リモートレジストリサービスが開始されている必要があります。「コントロール パネル」→「コントロール パネル ホーム」→「システムとメンテナンス」→「管理ツール」→「サービス」に移動し、リモートレジストリサービスを開始します。このサービスを「自動」に設定して、再起動時にサービスが自動的に開始されるように設定することもできます。

## サーバサービスの有効化（Windows 8）

Windows 8 システムでは、サーバサービスも開始されている必要があります。デフォルトでは、このサービスは開始されており、「自動」に設定されています。使用している特定のバージョンと設定において、このように設定されていることを確認してください。これは、「コントロール パネル」→「コントロール パネル ホーム」→「システムとメンテナンス」→「管理ツール」→「サービス」で確認できます。開始されていない場合は、サーバサービスを開始してください。

## ユーザアクセス制御（UAC）の設定

UAC を設定する必要があります。設定には、1）リモート UAC 設定の変更、2）UAC ポリシーの無効化という 2 つの方法があります。

### 方法 1: リモート UAC の設定

1)「管理者として実行」モードでレジストリーエディタ（regedit.exe）を開始し、必要であれば管理者承認を付与します。

2）HKEY_LOCAL_MACHINE ハイブに移動します。

3）SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System キーを開きます。

4）次のプロパティを指定して新しい DWORD（32 ビット）値を作成します。

名前 : LocalAccountTokenFilterPolicy
値 : 1

5）レジストリ エディターを閉じます。

警告 : DWORD（32 ビット）と QWORD（64 ビット）のデータタイプの値は、64 ビットバージョンの Windows ではメニューで隣り合わせに位置しています。そのため、間違ったデータタイプを選択するミスが発生しやすくなっています。データタイプは、DWORD（32 ビット）であることが必要です。QWORD（64 ビット）を選択して、値を 1 に設定しても、リモート UAC は有効になりません。

システムの再起動またはサーバサービスの再始動の要請には問題があります。一部のドキュメントで推奨されているのにもかかわらず、レジストリでリモート UAC を無効にすると、これはすぐに反映されて、Qualys のスキャン中に ADMIN$ へのリモートアクセスが許可されます。

### 方法 2: UAC ポリシーの無効化

次の手順に従います。

1）コントロールパネルを開きます。「ユーザーアカウントの追加または削除」をクリックします。

2）ユーザアカウントを選択します。ユーザアカウントの下のリンク「メインのユーザー アカウントのページに移動」をクリックします。

3)「ユーザーアカウントの変更」ページで、「セキュリティ設定の変更」をクリックします。

4)「ユーザー アカウント制御 (UAC) を有効にして、お使いのコンピュータをより安全にします」ページで、「ユーザー アカウント制御 (UAC) を使ってコンピュータの保護に役立たせる」チェックボックスをオフに（クリア）し、「OK」をクリックします。

5）コンピュータを再起動します。

# 付録 B -Windows NT ドメイン

NT ドメインを使用する場合、次のいずれかの方法により、リモートレジストリへの読み取りアクセスやその他最小限のドメインアクセスが可能な権限を持つアカウントを作成して設定できます。この手順に従ってアカウントを作成して設定した後は、前述のグループポリシーを設定することをお勧めします（Windows ドメインアカウントの設定を参照）。

## オプション 1 – 管理者グループの使用

グローバル管理者グループに新規のユーザアカウントを作成できます。このオプションは Windows NT ベースのドメインで使用できます。

アカウント作成および設定の手順 :

1）管理者権限を持つアカウントでドメインコントローラにログインします。

2）“ qualys_account ” という新しいユーザアカウントを作成します。

3）“ qualys_account ” を、“ Domain Admins ” というグローバルグループのメンバーにします。

4）グループのプロパティの “ Member of ” 項で、“ Domain Admins ” グループを除くすべてのグループを削除します。

グローバルグループ “ Domain Admins ” はリモートシステムへのアクセスに使用します。このグループが Windows NT ドメインのメンバーになると、各システムの “ Administrators ” というローカルグループに自動的に追加されます。

## オプション 2 – SetACL コマンドラインツールを使用してリモートで ACL を設定

SetACL などのコマンドラインツールを使用して、レジストリキーの権限の変更プロセスをリモートで自動化できます。このオプションは Windows NT ドメインで使用できます。

注記 — Windows Active Directory ドメインや別のバージョンの Windows を実行しているワークステーションといった一部の環境では、この方法により、特定のワークステーションのレジストリキーをリモートで設定できる場合があります。この場合、オプション 1 に従ってドメイン全体のポリシーを設定すると、レジストリキーは Windows 2000/2003/XP ワークステーション専用に設定されます。前のバージョンの Windows を実行しているワークステーションでは、これらのシステムのレジストリキーの変更には SetACL ツールを使用してください。

SetACL コマンドラインツールは http://setacl.sourceforge.net/ からダウンロードできます。

アカウント作成および設定の手順 :

1）管理者権限を持つアカウントでドメインコントローラにログインします。

2）“ qualys_scanners ” という新しいグローバルグループを作成します。

3）グループのプロパティで、グループにメンバーが存在しないことを確認します。

4）“ qualys_account ” という新しいユーザアカウントを作成し、“ qualys_scanners ” グループに追加します。

5）アカウントのプロパティの “ Member of ” 項で、“ Administrators ” を除くすべてのグループを削除します。

6) コマンドラインで SetACL を実行し、次の構文を使用して対象ホストのリモートアクセスレジストリキーを設定します。

```
setacl on "\\NETBIOS_NAME\MACHINE\SYSTEM\CurrentControlSet\Control\
SecurePipeServers\winreg"
-ot reg -actn ace -ace "n:DOMAIN\GROUPNAME;p:read;m:grant;w:dacl;i:np"
```

GROUPNAME は “ qualys_scanners ” グループ（作成したグローバルグループ）です。

# 付録 C - Windows 認証の QID

以下の脆弱性チェック（QID）からは、Windows の信頼できるスキャンの検証と、ログインに使用されるユーザアカウントのテストのための貴重な情報が返されます。

## Windows 認証のステータス

| QID | 重大度 | タイトル |
|---|---|---|
| 70053 | | ユーザ提供資格情報の Windows 認証のメソッド（Authentication Method for User-Provided Credentials） |
| 70028 | | Windows 認証のメソッド（Windows Authentication Method） |
| 105015 | | Windows 認証の失敗（Windows Authentication Failed） |
| 105296 | | Windows 認証が試行されない（Windows Authentication Not Attempted） |

## Windows 情報 — レジストリおよびファイルアクセス

| QID | 重大度 | タイトル |
|---|---|---|
| 70038 | | ファイルとプリンタへのアクセスが無効な脆弱性（File and Print Access Denied） |
| 90035 | | AllowedPaths レジストリキーが存在しない場合（Missing AllowedPaths Registry Key） |
| 90331 | | ファイル共有へのアクセスが有効な脆弱性（Access to File Share is Enabled） |
| 90399 | | 拒否された Windows ファイルへのアクセス（Windows File Access Denied） |
| 90194 | | Windows レジストリパイプのアクセスレベル（Windows Registry Pipe Access Level） |
| 90195 | | Windows レジストリキーへのアクセス拒否（Windows Registry Key Access Denied） |
| 105025 | | Windows におけるレジストリのアクセスレベル（Windows Registry Access Level） |
| 105177 | | Microsoft Windows のレジストリに重要なチェックのセキュリティポリシー（Microsoft Windows Registry Critical Checks Security Policy） |

# サポートへのお問い合わせ

Qualys は綿密なサポートを提供します。不明な点には、オンラインドキュメント、電話サポート、および E メールによる直接サポートを通じて、可能な限り迅速にお答えします。弊社は 24 時間年中無休でサポートを提供します。オンラインサポートの情報については、www.qualys.com/support/ をご覧ください。